



7 Times Square, New York, NY 10036-6569 Tel: 212-421-4100 Fax: 212-326-0806

New York | Los Angeles | Miami

pryorcashman.com

Sidhardha Kamaraju

Direct Tel: 212-326-0895
Direct Fax: 212-326-0806
skamaraju@pryorcashman.com

April 29, 2024

VIA EMAIL

Ryan Finkel, Esq.
Juliana Murray, Esq.
Micah Ferguson, Esq.
Justin Horton, Esq.
United States Attorney's Office
Southern District of New York
26 Federal Plaza
New York, NY 10007

Re: United States v. Kwok et al., Case No. 1:23-cr-00118 (AT)

Dear Counsel:

Pursuant to the Court's April 24, 2024, Order, Defendant Ho Wan Kwok provides this supplemental disclosure regarding the anticipated testimony of Paul Doran.

I. The Bases for Mr. Doran's Testimony

As described below, Mr. Doran will offer expert testimony about certain policies and tactics used by the Chinese Communist Party (the "CCP" or "the Party") to silence or censor political dissidents, including Mr. Kwok. As described in more detail in the curriculum vitae submitted with his initial disclosure, Mr. Doran's opinions are based on, among other things, his experience working for the British government and as a private security consultant for more than 25 years. In particular, Mr. Doran worked for the Foreign and Commonwealth Office (British equivalent of the State Department) for approximately three and a half years. During that time, Mr. Doran received training on the activities of the Chinese intelligence and police agencies, including a focus on their organization, methods and objectives when operating outside China and in pursuit of the policy goals of the CCP.

In addition to Mr. Doran's government service, he has also worked as a corporate risk professional for more than 20 years. Mr. Doran's time as a corporate risk professional included a four year period between 2012 and 2016 during which Mr. Doran resided in China and advised clients there about how to protect themselves against CCP targeting. Since that time, Mr. Doran has advised corporate and individual clients about, among other things, the risk associated with



April 29, 2024

Page 2

the CCP's targeting of its perceived political enemies, including its suppression of criticism expressed by Chinese dissidents or the regime's perceived political enemies.

Mr. Doran's experience includes consulting through Quintel Intelligence, an investigatory firm that specializes in, among other things, risk management. As part of Mr. Doran's work on behalf of Quintel, Mr. Doran advises clients about, among other things, the tactics and methods used by the CCP to target its perceived political enemies, and the security measures that clients might take to mitigate those risks.

II. Mr. Doran's Expert Opinions

Mr. Doran will offer the following expert opinions as part of his anticipated testimony:

1. The People's Republic of China (the "PRC" or "China") is a repressive dictatorship dominated by a single political party, the CCP. The Party regards any political dissent as a threat to its own political interests, but also to China's one-party system of government itself. The CCP directs the activities of the Chinese intelligence and law enforcement agencies to routinely monitor and suppress speech and activity inconsistent with CCP-approved viewpoints, as well as speech that threatens to damage the reputation of the CCP or to undermine the CCP's dictatorship. The CCP describes "Five Poisons," or beliefs, which it cannot tolerate at home or abroad. These "Five Poisons" are: (i) pro-democracy beliefs; (ii) religious groups or figures such as Falun Gong or the Dalai Lama; (iii) Taiwanese independence, (iv) Tibetan independence and (v) Xinjiang (or Uyghur) independence.
2. Operation FOX HUNT is a global "dirty tricks" campaign directed by Chinese President Xi Jinping and his subordinates in the CCP to target Chinese nationals living outside China whom the CCP sees as a political threat. This includes political dissidents and critics seeking to expose corruption in the CCP and human rights abuses in China (see also "the Five Poisons" outlined above). The CCP has identified and designated thousands of targets around the world for Operation FOX HUNT, including hundreds in the United States. Targets of Operation FOX HUNT are subject to surveillance, harassment and persecution using a variety of methods and techniques (outlined below).
3. United States law enforcement agencies such as the Federal Bureau of Investigation ("FBI"), including Director Christopher Wray, have spoken publicly about FOX HUNT. "China describes FOX HUNT as some kind of international anti-corruption campaign. It is not. Instead, FOX HUNT is a sweeping bid by [President] Xi to target Chinese nationals who he sees as threats and who live outside of China across the world. We are talking about political rivals, dissidents and critics seeking to expose China's extensive human rights violations."



April 29, 2024

Page 3

4. Operation FOX HUNT was launched in 2014 and is under the personal command of President Xi. Xi has delegated operational responsibility for executing FOX HUNT to the Chinese Ministry of Public Security (“MPS”) which is led by Wang Xiaohong. Ostensibly, the MPS oversees all of China’s domestic and foreign law enforcement activities and may be thought of as something like the US FBI. However, the MPS is also secret police force whose remit includes the monitoring and suppression of political dissidents. The MPS is supported in FOX HUNT by the Ministry of State Security (“MSS”) led by Chen Yixin. The MSS is China’s foreign intelligence agency, roughly the equivalent of the US Central Intelligence Agency (“CIA”). MSS officers under diplomatic cover in the US cooperate with the MPS in operations against Operation FOX HUNT targets. The Chinese military’s Information Support Force (“ISF”) is a specialist cyber espionage agency which conducts computer network exploitation (“CNE”) or hacking operations against Chinese dissidents around the world in support of Operation FOX HUNT.
5. The MPS has created secret, extra-legal Chinese police stations (known as “Overseas 110” stations). There are or have been 47 such stations in at least 38 countries, including one station identified in New York City. These stations have been used as bases for MPS personnel to surveil, harass and intimidate Chinese dissidents.
6. The CCP chooses its targets for Operation FOX HUNT based on monitoring of the online and other political activities of Chinese dissidents. It particularly targets dissidents who have large social media followings or access to media platforms including traditional broadcast and print media, but also outlets such as YouTube and other self-broadcast media, and who use this access to highlight corruption in the CCP and human rights abuses in China.
7. Tactics employed by the MPS to surveil, harass, intimidate and threaten dissidents include the following:
 - a. Threats to imprison, harm, rape or even kill dissidents’ family members who may still be in China or Hong Kong.
 - b. Forcibly dividing families by preventing dissidents’ family members from leaving China in the hope this will force dissidents to return to China.
 - c. Conducting Computer Network Exploitation (“CNE”) operations against dissidents. CNE includes enabling actions and intelligence gathering via computer networks and smart phones using a variety of techniques to gather data from the targets’ computers or engage in disruptive online activity against them. Encompassed within CNE are the following:



April 29, 2024

Page 4

- i. Spearphishing: This is a targeted attempt to steal sensitive information such as account credentials (“credential harvesting”) from a specific victim for malicious reasons. Typically, this is done through tricking the victim into opening malware sent to them by email or SMS which then deploys a “payload” to penetrate the victim’s private online presence.
- ii. Doxing or doxxing: This is the act of publicly providing personally identifiable information about an individual or organization, usually via the Internet and without their consent. Information might be sensitive or embarrassing in nature and exposing it is intended to blackmail the victim or else cause him or her psychological harm.
- iii. Denial of service (DoS) attacks: a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network.
- iv. Online disinformation campaigns also known as "spamouflage" and sometimes as “Dragonbridge”: these campaigns use fictitious social media accounts and automated “spambots” to flood the Internet with false and damaging information about the victim, for example, falsely accusing them of crimes or of embarrassing personal conduct. Online disinformation campaigns increasingly use AI-generated deepfakes to create damaging stories about victims.
- d. Hacking into major telecommunication companies in an effort to spy on users including in the US.
- e. Freezing of financial assets and de-banking in China and Hong Kong, which can have a knock-on effect for dissidents overseas as their local banks may see the Chinese de-banking as indication of criminal behavior and may then also withdraw their banking services from the victim.
- f. Filing of lawsuits against Chinese dissidents that make false accusations against them.
- g. Accusations of criminal wrongdoing and abuse of Interpol “red notices” to compel host countries to arrest dissidents on China’s behalf. Being the subject of a “red notice” may also create reputational damage for the victim as such notices are often taken as indications that the subject has engaged in criminal activities or behavior, which may not be the case with FOX HUNT targets.



April 29, 2024

Page 5

- h. Surveillance and physical harassment of dissidents by Chinese agents in the countries in which the dissidents live.
- i. Kidnapping, sometimes with the connivance of the host government if that government is aligned with China or seeking to appease the CCP.
- j. As part of its broader efforts to influence opinion in foreign countries, enhance its own standing and de-legitimize Chinese dissidents abroad, the CCP directs the MSS and other Chinese intelligence agencies to recruit or attempt to recruit local nationals and then directs them to apply for jobs at local, state and federal agencies. Should the local national sent by the CCP succeed in finding roles in those agencies they would act secretly and corruptly on behalf of the CCP. Acting as so-called "agents of influence", they would secretly promote the CCP's aims and objectives, including denigrating and de-legitimizing Chinese dissidents.¹
8. The US Department of Justice (DoJ) and the FBI have acted against Chinese police and intelligence agents conducting FOX HUNT operations in the US. These actions have included counterintelligence operations to prevent and disrupt Chinese police, and intelligence activities on US territory targeting dissidents. Such activities fall under the DoJ and FBI's remit to counter "transnational repression" (defined by the FBI as "when foreign governments harass and intimidate their own citizens living in the U.S. These governments may also target naturalized or U.S.-born citizens who have family overseas or other foreign connections. This violates U.S. law and individual rights and freedoms.").²
9. DoJ charging documents issued against Chinese agents and their US hirelings make direct and indirect references to Operation FOX HUNT. In particular, the US Department of Justice has brought criminal charges against numerous individuals for targeting Ho Kwan Kwok, also known as Miles Guo or Miles Kwok, for participating in the "912 Special Project Working Group", a specially designated group of Chinese government operatives tasked with harassing and attempting to censor Mr. Kwok online as part of Operation FOX HUNT. According to the DoJ, as part of this effort the CCP has also sought to bully US social media companies into censoring Mr. Kwok and have tried to "forcibly repatriate" Mr. Kwok back to China where he would undoubtedly face persecution, imprisonment and no access to a fair trial.

¹ See for example the case of Kun Shan Chun, a former employee of the US Federal Bureau of Investigation (FBI): <https://www.justice.gov/opa/pr/fbi-employee-pleads-guilty-acting-united-states-agent-chinese-government>.

² <https://www.fbi.gov/investigate/counterintelligence/transnational-repression>.



April 29, 2024

Page 6

10. Countries allied to the United States have also taken measures to combat illegal Chinese intelligence operations in their countries through new national security legislation, including:
 - a. Australia: In June 2018, Australia introduced the National Security Amendment (Espionage and Foreign Interference) Act 2018 (“EFI Act”) to combat the growing challenge of foreign interference in Australia, including that done by China.
 - b. Canada: The Security of Information Act 1985 is currently the subject of a high-level review which will seek to update legislation to account for new techniques of foreign interference in Canada by states including China.
 - c. Singapore: The 2021 Foreign Interference (Countermeasures) Act grants the government new powers to investigate individuals suspected of engaging in interference and disinformation campaigns on behalf of foreign states, including China.
 - d. United Kingdom: The National Security Act 2023 creates several measures to enable UK law enforcement and intelligence agencies to detect, deter and disrupt the full range of modern-day state threats including malign interference by countries including China.

III. Reservation of Rights to Supplement

As noted above, the government continues to produce discovery and, accordingly, Mr. Doran’s review and analysis is ongoing. Mr. Doran reserves the right to supplement and/or amend these disclosures, including in response to the government’s disclosures and the evidence presented in its case-in-chief.



April 29, 2024

Page 7

Very truly yours,

A handwritten signature in blue ink, appearing to read "Sidhardha Kamaraju".

PRYOR CASHMAN LLP
Sidhardha Kamaraju
E. Scott Schirick
Matthew S. Barkan
Daniel J. Pohlman
Clare P. Tilton

Reviewed, Approved, and Adopted by:

A handwritten signature in blue ink, appearing to read "Paul Doran".

Paul Doran